

Exam Questions SPLK-1005

Splunk Cloud Certified Admin

<https://www.2passeasy.com/dumps/SPLK-1005/>



NEW QUESTION 1

What is the default value of the LINE_BREAKER setting that splits the incoming stream of data into separate lines?

- A. Any sequence of newlines and carriage returns
- B. Any sequence of spaces and tabs
- C. Any sequence of punctuation marks
- D. Any sequence of alphanumeric characters

Answer: A

NEW QUESTION 2

What are the four default roles that Splunk Cloud Platform comes with?

- A. admin, power, user, can_delete
- B. admin, power, user, sc_admin
- C. admin, power, user, guest
- D. admin, power, user, can_write

Answer: B

NEW QUESTION 3

What is the name of the attribute that specifies the sed script for data transformation in the props.conf file?

- A. SEDCMD
- B. FORMAT
- C. DEST_KEY
- D. TRANSFORMS

Answer: A

NEW QUESTION 4

What is the name of the attribute that you need to set to true in the [search] stanza of the limits.conf file to enable Data Preview?

- A. timeline_events_preview
- B. data_preview_enabled
- C. show_data_preview
- D. enable_data_preview

Answer: A

NEW QUESTION 5

Which feature of forwarders can protect the data from unauthorized access or tampering?

- A. Data compression
- B. SSL security
- C. Data masking
- D. Data encryption

Answer: B

NEW QUESTION 6

What is the name of the configuration file where you can define data transformations using regular expressions and other attributes?

- A. limits.conf
- B. props.conf
- C. inputs.conf
- D. transforms.conf

Answer: D

NEW QUESTION 7

Which configuration file parameter can be used to modify line termination settings interactively, using the Set Source Type page in Splunk Web?

- A. LINE_BREAKER
- B. SHOULD_LINEMERGE
- C. BREAK_ONLY_BEFORE
- D. TRUNCATE

Answer: B

NEW QUESTION 8

Which configuration file needs to be edited to enable local indexing on the forwarder?

- A. outputs.conf
- B. inputs.conf
- C. props.conf
- D. transforms.conf

Answer: A

NEW QUESTION 9

Which setting in inputs.conf can be used to specify the SSL certificate for a TCP or UDP input?

- A. sslCertPath
- B. sslRootCAPath
- C. sslPassword
- D. All of the above

Answer: D

NEW QUESTION 10

What is the name of the default field that stores the timestamps in UNIX time when data is indexed?

- A. _time
- B. _timestamp
- C. _date
- D. _epoch

Answer: A

NEW QUESTION 10

Which feature allows a heavy forwarder to route data to different indexers based on criteria such as source, sourcetype, or host?

- A. Data cloning
- B. Data filtering
- C. Data sampling
- D. Data masking

Answer: A

NEW QUESTION 13

Which type of forwarder is a full Splunk Enterprise instance that can run apps and add-ons?

- A. Universal forwarder
- B. Heavy forwarder
- C. Deployment server
- D. Search head

Answer: B

NEW QUESTION 16

What is the name of the configuration file where you can specify the source type for a data input?

- A. limits.conf
- B. props.conf
- C. inputs.conf
- D. transforms.conf

Answer: C

NEW QUESTION 19

What is the name of the Splunk Cloud setting that allows you to specify the maximum amount of raw data allowed before data is removed from the index?

- A. Max raw data size
- B. Max data retention
- C. Max index size
- D. Max data volume

Answer: A

NEW QUESTION 22

Which input type can be used to monitor Windows Registry Values for changes?

- A. WinRegMon
- B. WinRegistry
- C. WinRegValue
- D. WinRegChange

Answer: A

NEW QUESTION 25

What is the name of the Splunk Cloud feature that allows you to monitor and manage resource utilization by business units and users using a Splunk app?

- A. Splunk App for Chargeback
- B. Splunk App for Resource Management
- C. Splunk App for Usage Analytics
- D. Splunk App for Cost Optimization

Answer: A

NEW QUESTION 26

Which feature of forwarders can prevent data loss in case of network failure or congestion?

- A. Data compression
- B. SSL security
- C. Configurable buffering
- D. Persistent queues

Answer: D

NEW QUESTION 31

What is the main advantage of managed Splunk Cloud over self-service Splunk Cloud in terms of scalability and reliability?

- A. Managed Splunk Cloud provides a single-instance environment that can scale up to 10TB/day and offers a 100% uptime SLA.
- B. Managed Splunk Cloud provides a clustered environment that can scale up to 10TB/day and offers a 100% uptime SLA.
- C. Managed Splunk Cloud provides a single-instance environment that can scale up to 5TB/day and offers a 99.9% uptime SLA.
- D. Managed Splunk Cloud provides a clustered environment that can scale up to 5TB/day and offers a 99.9% uptime SLA.

Answer: B

NEW QUESTION 35

Which feature allows a light forwarder to reduce the amount of data sent to the indexer by discarding some events or fields?

- A. Data cloning
- B. Data filtering
- C. Data sampling
- D. Data masking

Answer: C

NEW QUESTION 36

What is the name of the process that breaks the stream of raw data into individual lines called events?

- A. Line breaking
- B. Event annotation
- C. Event transformation
- D. Timestamp extraction

Answer: A

NEW QUESTION 38

Which setting in inputs.conf can be used to set the host field to a static value for a monitor input?

- A. host
- B. host_regex
- C. host_segment
- D. host_override

Answer: A

NEW QUESTION 39

Which input type can be used to monitor Windows Event Logs from a remote machine?

- A. WinEventLog
- B. WinEventLogCollections
- C. WinEventLogForwarder
- D. WinEventLogRemote

Answer: B

NEW QUESTION 41

Which configuration file contains the settings for event line breaking and line merging?

- A. inputs.conf
- B. outputs.conf
- C. props.conf
- D. transforms.conf

Answer: C

NEW QUESTION 45

Which setting in inputs.conf can be used to specify the interval at which the script runs for a scripted input?

- A. interval
- B. frequency
- C. schedule
- D. cron

Answer: A

NEW QUESTION 50

Which type of forwarder can perform data parsing and enrichment before sending it to the indexer?

- A. Universal forwarder
- B. Heavy forwarder
- C. Deployment server
- D. Search head

Answer: B

NEW QUESTION 53

What is the name of the component that acts as a data manager and sends data to Splunk Cloud Platform indexers?

- A. Heavy forwarder
- B. Universal forwarder
- C. Deployment server
- D. License master

Answer: A

NEW QUESTION 57

Which option can be used to specify the host value of the data when creating a file or directory monitor input?

- A. Set Host
- B. Select Host
- C. Choose Host
- D. Define Host

Answer: A

NEW QUESTION 61

What is the name of the input processor that allows you to monitor files that Windows rotates automatically on machines that run Windows Vista or Windows Server 2008 and higher?

- A. monitor
- B. MonitorNoHandle
- C. upload
- D. UploadNoHandle

Answer: B

NEW QUESTION 64

Which file processor can be used to index files that are locked by another process on Windows systems?

- A. Monitor
- B. MonitornoHandle
- C. Upload
- D. None of the above

Answer: B

NEW QUESTION 67

Which Splunk add-on simplifies the process of getting data into Splunk Cloud Platform from Windows Event Log channels?

- A. Splunk Add-on for Windows
- B. Splunk Add-on for Infrastructure
- C. Splunk Add-on for Active Directory
- D. Splunk Add-on for DNS

Answer: A

NEW QUESTION 71

Which feature of forwarders can improve the network performance and reduce the bandwidth consumption?

- A. Data compression
- B. SSL security
- C. Data sampling
- D. Data filtering

Answer: A

NEW QUESTION 74

What is the name of the configuration file that you need to edit to enable Data Preview for the search app?

- A. limits.conf
- B. props.conf
- C. inputs.conf
- D. outputs.conf

Answer: A

NEW QUESTION 78

What is the name of the Splunk Cloud feature that allows you to perform self-service administrative tasks such as creating indexes, inputs, and roles?

- A. Admin Config Service
- B. Admin Console
- C. Admin Dashboard
- D. Admin Toolkit

Answer: A

NEW QUESTION 83

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SPLK-1005 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SPLK-1005 Product From:

<https://www.2passeasy.com/dumps/SPLK-1005/>

Money Back Guarantee

SPLK-1005 Practice Exam Features:

- * SPLK-1005 Questions and Answers Updated Frequently
- * SPLK-1005 Practice Questions Verified by Expert Senior Certified Staff
- * SPLK-1005 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SPLK-1005 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year